Amendments to the Claims:

The following listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) An access privilege transferring method for safely transferring access privileges between clients, and between clients and servers, over an object space in which at least one server for providing objects and at least one client requiring the objects are connected to one another by a network, and access to each of the objects complying with privilege information held by each of the clients is allowed, comprising:

holding user information and secret information by each of a plurality of clients;

holding, in a server, the user information and the secret information of at least a first of the plurality of clients;

generating privilege information by the at least the first of the plurality of clients;

applying a predetermined calculating operation to information comprising at least the privilege information and the secret information, thereby generating protected privilege information; by the at least the first of the plurality of clients;

transmitting the user information, the privilege information and the protected privilege information from the at least the first of the plurality of clients to at least a second of the plurality of clients;

retransmitting, from the at least the second of the plurality of clients, the user information, the privilege information and the protected privilege information to the server, thereby making a request to access an object;

checking, by the server, whether the privilege information received from the at least the second of the plurality of clients is valid;

applying a predetermined calculating operation to information comprising at least the privilege information and the secret information, thereby generating protected privilege information by the server;

comparing the protected privilege information received by the server with the protected privilege information generated by the server; and

allowing access to an object in response to the coincidence of the received protected privilege information and the generated protected privilege information based on the results of the comparison.

2.   (Previously Presented) The access privilege transferring method according to claim 1, wherein the at least the second of the plurality of clients retransmits the user information, the privilege information and the protected privilege information to at least a third of the plurality of clients.

3.   (Previously Presented) An access privilege transferring method for allowing each of the clients activated over an object space in which at least one server for providing objects and at least one client requiring the objects are connected to one another by a network and access to each of the objects complying with privilege information held by each of the clients is allowed to safely transfer access privileges to another client, comprising:

holding user information and secret information to be shared by at least one server;

generating privilege information; and

applying a predetermined calculating operation to information comprising at least the privilege information and the secret information, thereby generating protected privilege information to be safely transferred to a client.

4.   (Previously Presented) An access privilege transferring method for allowing each of the servers activated over an object space in which at least one server for providing

objects and at least one client requiring the objects are connected to one another by a network and access to each of the objects based on privilege information held by each of the clients is allowed to safely respond to an access request issued from the client to which access privileges are transferred, comprising:

receiving an access request including user information, privilege information and protected privilege information;

checking whether the received privilege information is valid;

applying a predetermined calculating operation to information comprising at least the privilege information and the secret information, thereby generating protected privilege information;

comparing the received protected privilege information with the generated protected privilege information; and

allowing access to an object in response to the coincidence of the received protected privilege information and the generated protected privilege information based on the results of the comparison.

5.   (Previously Presented) The access privilege transferring method according to claim 1, wherein applying a predetermined calculating operation further comprises applying a one-way function to a bit string obtained by concatenating operands with one another.

6.   (Previously Presented) An access privilege transferring method for safely transferring access privileges between clients, and between clients and servers, over an object space in which at least one server for providing objects and at least one client requiring the objects are connected to one another by a network and access to each of the objects complying with privilege information held by each of the clients is allowed, comprising:

holding user information and secret information by each of a plurality of clients;

holding, in a server, the user information and the secret information of at least a first of the plurality of clients;

generating privilege information by the at least the first of the plurality of clients;

applying a predetermined calculating operation to information comprising at least the privilege information and the secret information, thereby generating first protected privilege information by the at least the first of the plurality of clients;

transmitting the user information, the privilege information and the first protected privilege information from the at least the first of the plurality of clients to at least a second of the plurality of clients;

receiving, by the at least the second of the plurality clients, a challenge character string from the server;

applying the predetermined calculating operation to information comprising at least the challenge character string and the first protected privilege information, thereby generating second protected privilege information by the at least the second of the plurality clients;

transmitting the user information, the privilege information and the second protected privilege information from the at least the second of the plurality clients to the server, thereby making a request to access an object;

checking, by the server, whether the privilege information received by the server is valid;

applying the predetermined calculating operation to information comprising at least the privilege information and the secret information, thereby generating first protected privilege information by the server;

applying the predetermined calculating operation to information comprising at least the challenge character string and the generated first protected privilege information, thereby generating second protected privilege information;

comparing the received second protected privilege information with the generated second protected privilege information; and

allowing access to the object in response to the coincidence of the received second protected privilege information and the generated second protected privilege information based on the results of the comparison.

7.   (Currently Amended) The access privilege transferring method according to claim 6, wherein the at least the second of the plurality of clients retransmits the user information, the privilege information and the second protected privilege information at least a third of the plurality of clients.

8.   (Previously Presented) An access privilege transferring method for safely transferring access privileges between clients and servers to which user information, privilege information and first protected privilege information are transferred, over an object space in which at least one server for providing objects and at least one client requiring the objects are connected to one another by a network and access to each of the objects complying with privilege information held by each of the clients is allowed, comprising:

transmitting a challenge character string from the server to a client that makes a request to access an object;

applying a predetermined calculating operation to information comprising at least the challenge character string and first protected privilege information, thereby generating second protected privilege information by the client;

retransmitting, by the client, user information, the privilege information and the second protected privilege information to a server, thereby making a request to access an object;

checking, by the server, whether the privilege information received by the server is valid;

applying the predetermined calculating operation to information comprising at least the privilege information and secret information, thereby generating first protected privilege information by the server.

applying the predetermined calculating operation to information comprising at least the challenge character string and the first protected privilege information generated by the server, thereby generating second protected privilege information by the server;

comparing, in the server, the second protected privilege information received and checked by the server with the second protected privilege information generated by the server; and

allowing access to an object by the server in response to the coincidence of the received second protected privilege information and the generated second protected privilege information based on the results of the comparison.

9.   (Previously Presented) The access privilege transferring method according to claim 6, wherein applying a predetermined calculating operation further comprises applying a one-way function to a bit string obtained by concatenating operands with one another.

10.   (Currently Amended) An access privilege transferring method for safely transferring access privileges between clients, and between clients and servers, over an object space in which at least one server for providing objects and at least one client requiring the objects are connected to one another by a network and access to each of the objects complying with privilege information held by each of the clients is allowed, comprising:

holding user information and secret by each of a plurality of clients;

holding, in a server, the user information and the secret information of at least a first of the plurality of clients;

generating privilege information by the at least the first of the plurality of clients;

encrypting the generated privilege information by ~~using~~ applying a predetermined calculating operation to information comprising at least the generated privilege information and the secret information, thereby generating protected privilege information by the at least the first of the plurality of clients;

transmitting, from the at least the first of the plurality of clients; the user information and the protected privilege information to at least a second of the plurality of clients;

retransmitting, by the at least the second of the plurality of clients, the user information and the protected privilege information to the server, thereby making a request to access an object;

decrypting the protected privilege information by using the secret information corresponding to the user information, thereby generating privilege information by the server;

checking, by the server, whether the privilege information generated by the server is valid; and

allowing access to an object in accordance with the result of the validity check.

11-12. (Canceled)

13.   (Currently Amended) An access privilege transferring method for safely transferring access privileges between clients, and between clients and servers, over an object space in which at least one server for providing objects and at least one client requiring the

objects are connected to one another by a network and access to each of the objects complying with privilege information held by each of the clients is allowed, comprising:

holding user information and secret information by each of a plurality of clients;

holding, in the server, the user information and the secret information of at least a first of the plurality of clients;

generating privilege information by the at least the first of the plurality of clients;

encrypting the generated privilege information by ~~using~~ applying a predetermined calculating operation to information comprising at least the generated privilege information and the secret information, thereby generating first protected privilege by the at least the first of the plurality of clients;

transmitting the user information, the privilege information and the first protected privilege information from the at least the first of the plurality of clients to at least a second of the plurality of clients;

receiving, by the at least the second of the plurality of clients, a challenge character string from the server,

encrypting the challenge character string by ~~using~~ applying the predetermined calculating operation to information comprising at least challenge character string and the first protected privilege information, thereby generating second protected privilege information by the at least the second of the plurality of clients;

retransmitting, by the at least the second of the plurality of clients, the user information, the privilege information and the second protected privilege information to the server, thereby making a request to access an object;

checking, by the server, whether the privilege information received by the server is valid;

encrypting the privilege information by ~~using~~ applying a predetermined calculating operation to information comprising at least the privilege information and the secret information, thereby generating first protected privilege information by the server;

encrypting the challenge character string by ~~using~~ applying a predetermined calculating operation to information comprising at least the challenge character string and the first protected privilege information generated by the server, thereby generating second protected privilege information by the server;

comparing the received second protected privilege information with the generated second protected privilege information; and

allowing access to an object in response to the coincidence of the received second protected privilege information and the generated second protected privilege information based on the results of the comparison.

14.   (Currently Amended) An access transferring method for safely transferring access privileges between clients and servers to which user information, privilege information and first protected privilege information are transferred, over an object space in which at least one server for providing objects and at least one client requiring the objects are connected to one another by a network and access to each of the objects complying with privilege information held by the client is allowed, comprising:

transmitting a challenge character string to the client that makes a request to access an object;

encrypting the challenge character string by ~~using~~ applying a predetermined calculating operation to information comprising at least the challenge character string and the

first protected privilege information, thereby generating second protected privilege information;

transmitting the user information, the privilege information and the second protected privilege information to a server, thereby making a request to access an object;

checking whether the received privilege information is valid;

encrypting the privilege information by using applying a predetermined calculating operation to information comprising at least the privilege information and secret information, thereby generating first protected privilege information;

encrypting the challenge character string by using applying a predetermined calculating operation to information comprising at least the challenge character string and the generated first protected privilege information, thereby generating second protected privilege information;

comparing, in the server, the second protected privilege information received by the server with the second protected privilege information generated by the server; and

allowing access to an object by the server in response to the coincidence of the received second protected privilege information and the generated second protected privilege information based on the results of the comparison.

15-19. (Canceled)